CLAIM AMENDMENTS

1. (Currently Amended) An extremely secure method for a host processor to key a source content to a source storage medium to prevent use of an unauthorized copy of the source content comprising the host processor storing a fingerprinted content comprising the steps of:

determining a source fingerprint from the source storage medium, wherein the source fingerprint is a physical attribute of the source storage medium;

combining the source content to be secured with the source fingerprint to generate the fingerprinted content; and

instructing the source storage medium to store the fingerprinted content.

2. (Currently Amended) The extremely secure method of Claim 1 further comprising the step of a host processor reading and verifying the fingerprinted content, the reading and verifying step ~~-~~comprising the steps of:

instructing a local storage medium to read the fingerprinted content;

separating the source content to be secured from the source fingerprint;

requesting a local fingerprint from the local storage medium; and

comparing the local fingerprint with the source fingerprint and in response to the comparison determining whether to use the source content.

3. (Currently Amended) The extremely secure method of Claim 2 wherein the step of determining ~~requesting~~ a source fingerprint further comprises:

using an open protocol to request a secured communication from the source storage medium;

identifying a physical, statistically unique, verifiable and relatively immutable ~~characteristic~~ (PSUVI) characteristic associated with the source storage medium;

generating encryption and/or decryption keys;

returning the encryption key to the host processor;

using the encryption key to convert the source content to an encrypted protocol;

requesting from the source storage medium the PSUVI ~~fingerprint~~ characteristic; and

the source storage medium responding to the host processor with the PSUVI ~~fingerprint~~characteristic.

4. (Currently Amended) The extremely secure method of Claim 2 wherein the step of combining the source content with the source fingerprint to generate the fingerprinted ~~source~~ contents further comprises:

creating a hybrid content to be secured by combining the source content to be secured and the source fingerprint; and

encrypting the fingerprinted ~~source~~ content with an encryption key.

5. (Currently Amended) The extremely secure method of Claim 2 wherein the step of requesting a local fingerprint from the local storage medium further comprises the steps of:

requesting from the local storage storage medium a local ~~fingerprint~~ PSUVI characteristic;

replying to the host processor with the local ~~fingerprint~~ PSUVI characteristic; and

performing a secured verification of the local ~~fingerprint~~ PSUVI characteristic.

6. (Currently Amended) The extremely secure method of Claim 2 wherein the step of determining ~~requesting~~ a source fingerprint further comprises:

using an open protocol to request a secured communication from the source storage medium;

identifying a relatively mutable physical attribute (Non-PSUVI) characteristic associated with the source storage medium;

generating encryption and/or decryption keys;

returning the encryption key to the host processor;

using the encryption key to convert the source content to an encrypted protocol;

requesting from the source storage medium the non-PSUVI ~~fingerprint~~ characteristic; and

the source storage medium responding to the host processor with the non-PSUVI ~~fingerprint~~characteristic.

7. (Currently Amended) The extremely secure method of Claim 2 wherein the step of requesting a local fingerprint from the local storage medium further comprises the steps of:

requesting from the local storage medium a local ~~fingerprint~~ non-PSUVI characteristic;

replying to the host processor with the local ~~fingerprint~~ non-PSUVI characteristic; and

performing a secured verification of the local ~~fingerprint~~ non-PSUVI characteristic.

8. (Currently Amended) An extremely secure system to prevent use of an unauthorized copy of a source content on a storage medium comprising:

a host processor; and

a storage medium, the storage medium comprising a storage medium processor, -a host processor interface, a servo system, a read/write system, one or more storage disks, and an attribute detector to read a PSUVI characteristic from the one or more storage disks to use by the host processor to encrypt a source content to be secured.

9. (Currently Amended) An extremely secure system to prevent use of an unauthorized copy of a source content on a storage medium comprising:

a host processor; and

a storage medium, the storage medium comprising a storage medium processor, -a host processor interface, a servo system, a read/write system, one or more storage disks, and an attribute detector to read a non-PSUVI characteristic from the one or more storage disks to use by the host processor to encrypt a source content to be secured.

10. (Currently Amended) An extremely secure fingerprinted content of a storage medium, wherein the fingerprinted content comprises a source content to be secured combined with a fingerprint generated from a PSUVI characteristic of the storage medium.

11. (Currently Amended) An extremely secure fingerprinted content of a storage medium, wherein the fingerprinted content comprises a source content to be secured combined with a fingerprint generated from a non-PSUVI characteristic of the storage medium.

12. (New) The extremely secure method of Claim 1, wherein the source storage medium is a hard disk drive.

13. (New) The extremely secure method of Claim 12, wherein the source fingerprint is a defect list represented by physical block addresses.

14. (New) The extremely secure system of Claim 8, wherein the storage medium is a hard disk drive.

15. (New) The extremely secure system of Claim 14, wherein the PSUVI characteristic is a defect list represented by physical block addresses.

A5

16. (New) The extremely secure system of Claim 9, wherein the storage medium is a hard disk drive.

17. (New) The extremely secure system of Claim 16, wherein the non-PSUVI characteristic is a post-production defect list.

18. (New) The extremely secure fingerprinted content of Claim 10, wherein the storage medium is a hard disk drive.

19. (New) The extremely secure fingerprinted content of Claim 18, wherein the PSUVI characteristic is a defect list represented by physical block addresses.

20. (New) The extremely secure fingerprinted content of Claim 11, wherein the storage medium is a hard disk drive.

21. (New) The extremely secure fingerprinted content of Claim 20, wherein the the non-PSUVI characteristic is a post-production defect list.

22. (New) A method of securing source content from a hard disk drive, comprising:

providing a source content in a host processor;

providing a source fingerprint of a hard disk drive, wherein the source fingerprint is a physical attribute of the hard disk drive;

transferring the source fingerprint from the hard disk drive to the host processor; then

generating a fingerprinted source content in the host processor using the source content and the source fingerprint, wherein the fingerprinted source content represents the source content and the source fingerprint; then

transferring the fingerprinted source content from the host processor to the hard disk drive;

storing the fingerprinted source content in the hard disk drive; then

retransferring the fingerprinted source content from the hard disk drive to the host processor;

generating the source content and the source fingerprint from the retransferred fingerprinted source content in the host processor;

retransferring the source fingerprint from the hard disk drive to the host processor; and then

comparing the generated source fingerprint with the retransferred source fingerprint in the host processor, wherein the host processor determines whether the generated source content is sanctioned in response to the comparison.

23. (New) The method of Claim 22, wherein the source fingerprint is a statistically unique physical attribute of the hard disk drive.

24. (New) The method of Claim 23, wherein the source fingerprint is a relatively immutable physical attribute of the hard disk drive.

25. (New) The method of Claim 24, wherein the source fingerprint is a statistically unique, immutable and verifiable physical attribute of the hard disk drive.

26. (New) The method of Claim 22, wherein the source fingerprint is a detect list of the hard disk drive.

27. (New) The method of Claim 26, wherein the defect list includes physical block addresses.

28. (New) The method of Claim 22, wherein the source fingerprint is a servo characteristic of the hard disk drive.

29. (New) The method of Claim 28, wherein the servo characteristic is servo burst correction values.

A3

30. (New) The method of Claim 28, wherein the servo characteristic is servo burst correction value related repeatable runout response.

31. (New) The method of Claim 28, wherein the servo characteristic is servo wedge defects.

32. (New) The method of Claim 28, wherein the servo characteristic is a servo transfer function.

33. (New) The method of Claim 22, wherein the source fingerprint is a track misregistration behavior of the hard disk drive.

34. (New) The method of Claim 22, wherein the source fingerprint is a channel optimization of the hard disk drive.

35. (New) The method of Claim 34, wherein the channel optimization is a read channel optimization parameter related to an individual head.

36. (New) The method of Claim 34, wherein the channel optimization is a write channel optimization parameter related to an individual head.

37. (New) The method of Claim 22, wherein the source fingerprint is a statistically unique physical property of a head disk assembly of the hard disk drive.

38. (New) The method of Claim 22, wherein the source fingerprint is a statistically unique physical property of a printed circuit board of the hard disk drive.

39. (New) The method of Claim 22, wherein the source fingerprint is magnetic defects of the hard disk drive.

A5

40. (New) The method of Claim 22, wherein the source fingerprint is a head/media characteristic of the hard disk drive.

41. (New) The method of Claim 22, including transferring an encryption key from the hard disk drive to the host processor.

42. (New) The method of Claim 41, wherein generating the fingerprinted source content includes generating an encrypted source content using the source content and the encryption key in the host processor, and then generating the fingerprinted source content using the encrypted source content and the source fingerprint in the host processor.

43. (New) The method of Claim 41, wherein generating the fingerprinted source content includes generating a non-encrypted fingerprinted source content using the source content and the source fingerprint in the host processor, and then generating an encrypted fingerprinted source content using the non-encrypted fingerprinted source content and the encryption key.

44. (New) The method of Claim 22, wherein generating the fingerprinted source content includes encrypting the source content and the source fingerprint using an encryption algorithm.

45. (New) The method of Claim 22, wherein generating the source content includes decrypting the fingerprinted source content using a decryption algorithm.

46. (New) The method of Claim 22, wherein comparing the generated source fingerprint with the retransferred source fingerprint includes determining whether the generated source fingerprint and the retransferred source fingerprint match using statistical analysis.

47. (New) The method of Claim 46, wherein the statistical analysis includes determining whether a statistically large percentage of defects listed in the generated source fingerprint point to defects in the retransferred source fingerprint.

A5

48. (New) The method of Claim 46, wherein the statistical analysis includes determining whether a statistically small percentage of defects listed in the generated source fingerprint point to defects in the retransferred source fingerprint.

49. (New) The method of Claim 22, wherein the generated source content is enabled for use by the host processor if the generated source fingerprint matches the retransferred source fingerprint, and the generated source content is disabled for use by the host processor if the generated source fingerprint does not match the retransferred source fingerprint.

50. (New) The method of Claim 22, wherein the host processor uses the generated source content if the generated source fingerprint matches the retransferred source fingerprint, and the host processor does not use the generated source content if the generated source fingerprint does not match the retransferred source fingerprint.

51. (New) A method of securing source content from a hard disk drive, comprising:
providing a source content in a host processor;

providing a source fingerprint of a hard disk drive, wherein the source fingerprint is a physical, statistically unique, verifiable and relatively immutable (PSUVI) characteristic of the hard disk drive;

transferring the source fingerprint from the hard disk drive to the host processor; then

generating a fingerprinted source content in the host processor using the source content and the source fingerprint, wherein the fingerprinted source content represents the source content and the source fingerprint; then

transferring the fingerprinted source content from the host processor to the hard disk drive;

storing the fingerprinted source content in the hard disk drive; then

retransferring the fingerprinted source content from the hard disk drive to the host processor;

generating the source content and the source fingerprint from the retransferred fingerprinted source content in the host processor;

retransferring the source fingerprint from the hard disk drive to the host processor; and then

comparing the generated source fingerprint with the retransferred source fingerprint in the host processor, wherein the host processor determines whether the generated source content is sanctioned in response to the comparison.

52. (New) The method of Claim 51, wherein the source fingerprint is an immutable characteristic of the hard disk drive.

53. (New) The method of Claim 51, wherein the source fingerprint is a defect list.

54. (New) The method of Claim 51, including transferring an encryption key from the hard disk drive to the host processor.

55. (New) The method of Claim 54, wherein generating the fingerprinted source content includes generating an encrypted source content using the source content and the encryption key

in the host processor, and then generating the fingerprinted source content using the encrypted source content and the source fingerprint in the host processor.

56. (New) The method of Claim 54, wherein generating the fingerprinted source content includes generating a non-encrypted fingerprinted source content using the source content and the source fingerprint in the host processor, and then generating an encrypted fingerprinted source content using the non-encrypted fingerprinted source content and the encryption key.

57. (New) The method of Claim 51, wherein generating the fingerprinted source content includes encrypting the source content and the source fingerprint using an encryption algorithm.

58. (New) The method of Claim 51, wherein generating the source content includes decrypting the fingerprinted source content using a decryption algorithm.

59. (New) The method of Claim 51, wherein the generated source content is enabled for use by the host processor if the generated source fingerprint matches the retransferred source fingerprint, and the generated source content is disabled for use by the host processor if the generated source fingerprint does not match the retransferred source fingerprint.

60. (New) The method of Claim 51, wherein the host processor uses the generated source content if the generated source fingerprint matches the retransferred source fingerprint, and the host processor does not use the generated source content if the generated source fingerprint does not match the retransferred source fingerprint.

61. (New) A method of securing source content from a hard disk drive, comprising:
providing a source content in a host processor;
providing a media detect list of the hard disk drive;
transferring the media defect list from the hard disk drive to the host processor; then

generating a fingerprinted source content in the host processor using the source content and the media defect list, wherein the fingerprinted source content represents the source content and the source fingerprint; then

transferring the fingerprinted source content from the host processor to the hard disk drive;

storing the fingerprinted source content in the hard disk drive; then

retransferring the fingerprinted source content from the hard disk drive to the host processor;

generating the source content and the media detect list from the retransferred fingerprinted source content in the host processor;

retransferring the media defect list from the hard disk drive to the host processor; and then

comparing the generated media defect list with the retransferred media defect list in the host processor, wherein the host processor determines whether the generated source content is sanctioned in response to the comparison.

62. (New) The method of Claim 61, wherein the media defect list is a statistically unique, immutable and verifiable physical attribute of the hard disk drive.

63. (New) The method of Claim 61, wherein the media defect list includes physical block addresses.

64. (New) The method of Claim 61, including transferring an encryption key from the hard disk drive to the host processor.

65. (New) The method of Claim 64, wherein generating the fingerprinted source content includes generating an encrypted source content using the source content and the encryption key in the host processor, and then generating the fingerprinted source content using the encrypted source content and the media defect list in the host processor.

66. (New) The method of Claim 64, wherein generating the fingerprinted source content includes generating a non-encrypted fingerprinted source content using the source content and the media defect list in the host processor, and then generating an encrypted fingerprinted source content using the non-encrypted fingerprinted source content and the encryption key.

67. (New) The method of Claim 61, wherein generating the fingerprinted source content includes encrypting the source content and the media defect list using an encryption algorithm.

68. (New) The method of Claim 61, wherein generating the source content includes decrypting the fingerprinted source content using a decryption algorithm.

69. (New) The method of Claim 61, wherein the generated source content is enabled for use by the host processor if the generated media defect list matches the retransferred media defect list, and the generated source content is disabled for use by the host processor if the generated media defect list does not match the retransferred media defect list.

70. (New) The method of Claim 61, wherein the host processor uses the generated source content if the generated media defect list matches the retransferred media defect list, and the host processor does not use the generated source content if the generated media defect list does not match the retransferred media defect list.

71. (New) A method of securing source content from a hard disk drive, comprising:

providing a source content in a host processor;

providing a first source fingerprint of a first hard disk drive, wherein the first source fingerprint is a physical, statistically unique, verifiable and relatively immutable (PSUVI) characteristic of the first hard disk drive;

providing a second source fingerprint of a second hard disk drive, wherein the second source fingerprint is a physical, statistically unique, verifiable and relatively immutable (PSUVI) characteristic of the second hard disk drive;

transferring the first source fingerprint from the first hard disk drive to the host processor;

generating a fingerprinted source content in the host processor using the source content and the first source fingerprint, wherein the fingerprinted source content represents the source content and the first source fingerprint; then

transferring the fingerprinted source content from the host processor to a selected hard disk drive;

storing the fingerprinted source content in the selected hard disk drive; then

retransferring the fingerprinted source content from the selected hard disk drive to a host device;

generating the source content and the first source fingerprint from the retransferred fingerprinted source content in the host device;

transferring a selected source fingerprint from the selected hard disk drive to the host device, wherein the selected source fingerprint is the first source fingerprint if the selected hard disk drive is the first hard disk drive, and the selected source fingerprint is the second source fingerprint if the selected hard disk drive is the second hard disk drive; and then

comparing the generated source fingerprint with the selected source fingerprint in the host device, wherein the host device determines that the generated source content is sanctioned if the generated source fingerprint matches the selected source fingerprint, and the host device determines that the generated source content is unsanctioned if the generated source fingerprint does not match the selected source fingerprint.

72. (New) The method of Claim 71, wherein the first source fingerprint is an immutable characteristic of the first hard disk drive, and the second source fingerprint is an immutable characteristic of the second hard disk drive.

73. (New) The method of Claim 71, wherein the first source fingerprint is a first detect list of the first hard disk drive, and the second source fingerprint is a second detect list of the second hard disk drive.

74. (New) The method of Claim 73, wherein the first defect list includes first physical block addresses, and the second defect list includes second physical block addresses.

75. (New) The method of Claim 71, wherein the first source fingerprint is a first servo characteristic of the first hard disk drive, and the second source fingerprint is a second servo characteristic of the second hard disk drive.

76. (New) The method of Claim 75, wherein the first servo characteristic is first servo burst correction values, and the second servo characteristic is second servo burst correction values.

77. (New) The method of Claim 75, wherein the first servo characteristic is first servo burst correction value related repeatable runout response, and the second servo characteristic is second servo burst correction value related repeatable runout response.

78. (New) The method of Claim 75, wherein the first servo characteristic is first servo wedge defects, and the second servo characteristic is second servo wedge defects.

79. (New) The method of Claim 75, wherein the first servo characteristic is a first servo transfer function, and the second servo characteristic is a second servo transfer function.

80. (New) The method of Claim 71, wherein the first source fingerprint is a track misregistration behavior of the first hard disk drive, and the second source fingerprint is a track misregistration behavior of the second hard disk drive.

81. (New) The method of Claim 71, wherein the first source fingerprint is a first channel optimization of the first hard disk drive, and the second source fingerprint is a second channel optimization of the second hard disk drive.

82. (New) The method of Claim 81, wherein the first channel optimization is a read channel optimization parameter related to a first individual head, and the second channel optimization is a read channel optimization parameter related to a second individual head.

83. (New) The method of Claim 81, wherein the first channel optimization is a write channel optimization parameter related to a first individual head, and the second channel optimization is a write channel optimization parameter related to a second individual head.

84. (New) The method of Claim 71, wherein the first source fingerprint is a statistically unique physical property of a head disk assembly of the first hard disk drive, and the second source fingerprint is a statistically unique physical property of a head disk assembly of the second hard disk drive.

85. (New) The method of Claim 71, wherein the first source fingerprint is a statistically unique physical property of a printed circuit board of the first hard disk drive, and the second source fingerprint is a statistically unique physical property of a printed circuit board of the second hard disk drive.

86. (New) The method of Claim 71, wherein the first source fingerprint is magnetic defects of the first hard disk drive, and the second source fingerprint is magnetic defects of the second hard disk drive.

87. (New) The method of Claim 71, wherein the first source fingerprint is a head/media characteristic of the first hard disk drive, and the second source fingerprint is a head/media characteristic of the second hard disk drive.

88. (New) The method of Claim 71, including transferring an encryption key from the first hard disk drive to the host processor.

89. (New) The method of Claim 88, wherein generating the fingerprinted source content includes generating an encrypted source content using the source content and the encryption key in the host processor, and then generating the fingerprinted source content using the encrypted source content and the first source fingerprint in the host processor.

90. (New) The method of Claim 88, wherein generating the fingerprinted source content includes generating a non-encrypted fingerprinted source content using the source content and the first source fingerprint in the host processor, and then generating an encrypted fingerprinted source content using the non-encrypted fingerprinted source content and the encryption key.

91. (New) The method of Claim 71, wherein generating the fingerprinted source content includes encrypting the source content and the first source fingerprint using an encryption algorithm.

92. (New) The method of Claim 71, wherein generating the source content includes decrypting the fingerprinted source content using a decryption algorithm.

93. (New) The method of Claim 71, wherein the selected hard disk drive is the first hard disk drive, the selected source fingerprint is the first source fingerprint, and the host device determines that the generated source content is sanctioned.

94. (New) The method of Claim 93, wherein the host device is the host processor.

95. (New) The method of Claim 71, wherein the selected hard disk drive is the second hard disk drive, the selected source fingerprint is the second source fingerprint, and the host device determines that the generated source content is unsanctioned.

96. (New) The method of Claim 95, wherein the host device is another processor.

97. (New) The method of Claim 95, wherein transferring the fingerprinted source content from the host processor to the second hard disk drive includes transferring the fingerprinted source content from the host processor to the first hard disk drive, and then transferring the fingerprinted source content from the first hard disk drive to the second hard disk drive.

98. (New) The method of Claim 97, wherein transferring the fingerprinted source content from the first hard disk drive to the second hard disk drive includes transferring a drive image copy of the fingerprinted source content from the first hard disk drive to the second hard disk drive.

99. (New) The method of Claim 97, wherein transferring the fingerprinted source content from the first hard disk drive to the second hard disk drive is performed using low-level block copy software.

100. (New) The method of Claim 97, wherein the host device is another processor.

101. (New) The method of Claim 71, wherein the host device is the host processor.

A5

102. (New) The method of Claim 71, wherein the host device is another processor.

103. (New) The method of Claim 71, wherein comparing the generated source fingerprint with the selected source fingerprint includes determining whether the generated source fingerprint and the selected source fingerprint match using statistical analysis.

104. (New) The method of Claim 103, wherein the statistical analysis includes determining whether a statistically large percentage of items listed in the generated source fingerprint are consistent with the selected source fingerprint.

105. (New) The method of Claim 103, wherein the statistical analysis includes determining whether a statistically small percentage of items listed in the generated source fingerprint are inconsistent with the selected source fingerprint.

106. (New) The method of Claim 103, wherein the statistical analysis includes determining whether a statistically large percentage of defects listed in the generated source fingerprint point to defects in the selected source fingerprint.

107. (New) The method of Claim 103, wherein the statistical analysis includes determining whether a statistically small percentage of defects listed in the generated source fingerprint point to defects in the selected source fingerprint.

108. (New) The method of Claim 71, wherein the generated source content is enabled for use by the host device if the generated source fingerprint matches the selected source fingerprint, and the generated source content is disabled for use by the host device if the generated source fingerprint does not match the selected source fingerprint.

109. (New) The method of Claim 71, wherein the host device uses the generated source content if the generated source fingerprint matches the selected source fingerprint, and the host device does not use the generated source content if the generated source fingerprint does not match the selected source fingerprint.

110. (New) The method of Claim 71, wherein the host device determines that the generated source content is an authorized copy of the source content if the generated source fingerprint matches the selected source fingerprint, and the host device determines that the generated source content is an unauthorized copy of the source content if the generated source fingerprint does not match the selected source fingerprint.